A strategy for Identifying, Analyzing Cloud-Specific Threats (March 2, 2011)

1. Underlying Theme:
   (a) Many of the threats to the resources of the data center that the cloud provider owns/operates are well known and well documented.
   (b) Hence to address cloud-specific Threats, one has to focus on the vulnerabilities in Service Orchestration features

2. Classification of Threats:
   (a) Threats whose countermeasures are going to be identical whether the owner of the data center is a hosted service provider, enterprise or cloud service provider.
   (b) Threats whose countermeasures have to implemented differently due to the way in which the cloud service is orchestrated (e.g., patch management on rented VM instances)
   (c) Threats that are cloud-specific (e.g., side channel attacks by VMs owned by a rogue subscriber) which need tailored counter measures.

3. Strategy for Threat Identification & Analysis:
   (a) Identify functional capabilities in each layer of Security Services Architecture.
   (b) Identify sources of Threat from each functional capability in each of the layers.
   (c) Classify the threats into three categories in (2) above based on the security services that can act as the countermeasure for each.